

09/913690
531 Rec'd PCT 16 AUG 2001

National Phase of PCT/EP99/09980 in U.S.A.

Title: Method and Apparatus for Generating a Data Stream and
Method and Apparatus for Playing a Data Stream

Applicants: RUMP, Niels et al.

Translation of PCT Application PCT/EP99/09980
as originally filed

5 **Method and Apparatus for Generating a Data Stream and
Method and Apparatus for Playing a Data Stream**

Description

10 The present invention relates to the encryption or decryption of payload data, like e.g. audio and/or video data and especially to audio and/or video data present in the form of a data stream comprising a header and a payload data block.

15 With the occurrence of telecommunication networks and in particular due to the huge spreading of multimedia data-capable personal computers and, most recently, of so-called solid state players, a need has arisen to market digital
20 multimedia data, such as digital audio data and/or digital video data, commercially. Telecommunication networks for example can be analog telephone lines, digital telephone lines, such as ISDN, or the Internet. Among the commercial providers of multimedia products there is a need to sell or
25 lend multimedia data, wherein it should be possible for a costumer to be able to select a certain product individually at any time from a certain catalogue, this product then of course being only allowed to be used by the costumer who has paid for it.

30 Unlike well-known encrypted television programs, such as the television channel Premiere, in which the emitted data is encrypted in the same way for all users who have acquired a suitable decryption device by paying a certain
35 charge, the present invention is to provide methods and devices enabling an individual, customer-selective and safe encryption and decryption of multimedia data. Unlike the

5 television channels mentioned above which give a fixed pro-
gram all of which the user has to decide for, the methods
and devices of the present invention enable a maximum free-
dom of selection for the user, which means that the user
has only to pay for those products he or she actually wants
10 to use.

DE 196 25 635 C1 describes methods and devices for encrypt-
ing and decrypting multimedia data, the multimedia data be-
ing present in the form of an encrypted multimedia file
15 comprising a destination data block and a payload data
block. Parts of the destination data block and at least
some parts of the payload data block are encrypted by means
of different keys, especially symmetrical encryption meth-
ods being used.

20 Further, in the method for encrypting or decrypting multi-
media data described in DE 196 256 35 C1 a user index is
entered into a determination data block of a bitstream with
encrypted multimedia data that identifies the user author-
25 ized to use an encrypted multimedia data stream. If this
user index identifies merely one person, this method is
only safe against unauthorized copying if that person who
has purchased an encrypted multimedia data stream acts cor-
rectly and legally. This can, however, not always be guar-
30 anteed. If the person who has purchased an encrypted
multimedia data stream legally carries out copying, it will
not be possible to see from a copy who has copied it. The
origin of the copy can therefore not be tracked down
anymore which will open the way for violations of
35 copyrights, incorrect behaviour assumed.

5 However, if the user index does , not only identify the user as a person but a specific player of a user, like e.g. the PC of the user, a safety is achieved in such a way that the user can play the encrypted multimedia data stream only on the player identified by the user index regardless
10 whether the user behaves legally or illegally.

However, the problem with this solution is the fact that it is not flexible, i.e. it dictates the user where he has to play the purchased multimedia data stream due to the copy-
15 right protection. There is not a lot of imagination needed to predict that such system will only find little acceptance at the market especially when thinking about the fact that a number of players exist in a normal household. Such players can include for example a personal computer, a lap-
20 top, a hifi system, a car hifi system, a video recorder, a solid state player, etc.

Therefore, it is the object of the present invention to provide a flexible concept for selectively providing multi-
25 media data that on the one hand finds acceptance at the market and at the other hand takes copyright aspects into consideration.

This object is achieved by a method for generating a second
30 data stream from a first data stream according to claim 1, by a method for playing a second data stream generated based on a first data stream according to claim 15, by an apparatus for generating a second data stream from a first data stream according to claim 19, and by an apparatus for
35 playing a second data stream generated based on a first data stream according to claim 21.

5 The present invention is based on the knowledge that music piracy can only be limited by using a device-specific identification of payload data streams. This means that a payload data piece that has been processed in the form of a payload data stream is not licensed person-specific but device-specific. In order for such a system to find acceptance at the market the situation has to be taken into account that a person usually has several players and that a person wants to have a free choice on which player she/he wants to play the purchased multimedia piece.

15 It is pointed out at this stage that payload data in general includes multimedia data that is audio data, video data or a combination of audio data and video data, but also text data. For practical reasons the subject matter of the present invention will be disclosed using multimedia data. It is however clear that all the payload data for which there is a demand to follow up their origin can be processed by the devices and methods according to the invention.

25 However, to prevent the way from being opened again for unlimited copying, a "copy" of the multimedia data stream has to be carried out device-specific for another device of a user as well. At the same time it is absolutely significant that the origin of each copy of a multimedia piece can be tracked down, i.e. it should always be possible to ascertain without doubt who has created a multimedia piece (author, composer), who has put it into circulation (provider, distributor, supplier), who has made an intermediate copy, and who has possibly made a further intermediate copy, etc. Only when the origin is known a user of a multimedia piece can prove without doubt that he uses the multi-

5 media piece legally, or only then an illegal user can be found guilty without doubt.

Furthermore it is possible to carry out the binding of the multimedia data not to one player directly, but to bind the
10 data to a "Smart Card". Thereby identical multimedia data streams can be maintained on various devices, but can only be used on the respective device where the Smart Card is inserted at that time.

15 Therefore, according to the present invention a second data stream is generated from a first data stream comprising a first payload data block with multimedia data, that also comprises a first header and a first payload data block with multimedia data, a second data stream is generated
20 that also comprises again a header and a payload data block. However, in this second header, i.e. the header of the second data stream according to the present invention at least those parts of the first header, i.e. the header of the first data stream allowing conclusions as to the
25 origin of the multimedia data are included. The second payload data block comprises the same multimedia data as the first payload data block, i.e. the payload data block of the first data stream.

30 The header of the second data stream can essentially have the same format as the header of the first data stream. However, it includes Besides the usual header information comprises additionally at least the information from the first header allowing conclusions as to the origin of the
35 multimedia data.

5 Essentially, in a preferred embodiment of the present invention, the whole first header is entered into the second header. In order to protect the second header comprising the first header from manipulation it can additionally be provided with a digital signature that is derived from the
10 data of the second (current) header and above that from the data of the first (old) header. In a preferred embodiment of the present invention, data from the first header allowing conclusions as to the origin of the multimedia data comprise a supplier identification, i.e. an identification
15 of the supplier of the first data stream that could for example be the Deutsche Telekom (German telecommunications company), as well as author information allowing conclusions as to the author or composer, as well as a user identification, i.e. an identification of the device for which
20 the data stream has originally been licensed.

It is a specific advantage of the inventive concept that it can be carried out as often as desired what leads to a multiply recursive header structure since a third data stream
25 that comprises a third header and a third payload data block again comprises origin information of the second header in its header. This origin information is on the one hand the origin information of the first header and on the other hand the origin information of the second header.
30 Analogous to the origin information of the first header the origin information of the second header is for example an identification of the device the piece was originally licensed for by the original supplier and an identification of the device a "copy" was made for, for example an identification
35 of a car hifi system.

5 Here, it will be especially noted that the author information of the first header is also present in the header of the third data stream. Thus, the inventive concept is in conformity with statutory regulations regarding any program or any apparatus removing author information as illegal.
10 Such statutory regulations have already become national law in the United States and it might only be a question of time when these regulations will be nationalized Europe wide.

15 In a preferred embodiment of the present invention the part of an old header taken over into the new header contains only licensing information referring to the manner how a licensed multimedia piece may be used, i.e. how often it may be played and how often it may be copied or whether a
20 copy of a copy is legal or not.

The payload data block can of course be encrypted symmetrically, while the key of the symmetrical encrypting method is encrypted asymmetrically. In this case an apparatus for
25 generating the second data stream will carry out a complete decryption from the first data stream and subsequently a complete new encryption.

Thus, the inventive concept allows full protection of a
30 multimedia piece in a way from the author or composer via an arbitrary number of copies to an end user. Above that, the origin of a current copy can be tracked down unbrokenly at any time of a copy or distribution chain whereby the number of copies or distribution processes is arbitrary.
35 Additionally, author information is considered any time whereby copyright protection is satisfied. Finally, the inventive concept can be implemented efficiently and flexible

5 such that it is also suitable for inexpensive players with limited memory and processor resources, that it is easy to handle, and that modern client demands for high flexibility are fully considered.

10 Fig. 1 shows a multimedia data stream, which can be produced according to the present invention;

Fig. 2 shows a detailed illustration of the header and the payload data block of the encrypted multimedia data stream;

Fig. 3 shows a selection of certain entries into the individual sub blocks of the header block;

20 Fig. 4 a schematic illustration of a distribution sce-
nario;

Fig. 5 a schematic view of a data stream with recursive header structure;

Fig. 6 a flow chart of a method for generating a second data stream from a first data stream according to the present invention; and

30 Fig. 7 a method for playing a second data stream gener-
ated based on a first data stream according to
the present invention.

Fig. 1 shows an encrypted multimedia data stream 10 comprising a header 12 and a payload data block 14 that is a block containing encrypted multimedia data. The payload data block 14 includes encrypted sections 16 and unen-

5 encrypted sections 18 between the encrypted sections 16. In addition a multimedia data stream, which can be produced according to the present invention, includes a further un-encrypted section 20 following the header 12 and being arranged in front of an encrypted section 16.

10

Usually the multimedia data to be encrypted is encoded in any way, such as according to a MPEG standard, such as MPEG-2 AAC, MPEG-4 audio or MPEG Layer-3. It is thus sufficient to encrypt certain sections of the multimedia data to be encrypted. This leads to an essentially decreased processing expenditure both at the provider who encrypts the data and at the customer who in turn has to decrypt the data. Furthermore, the pleasure of hearing and seeing respectively of a user who only uses the unencrypted multimedia data is seriously impaired by the constantly occurring encrypted blocks, when the multimedia data is only encrypted partly.

Although Fig. 1 shows an encrypted multimedia data stream in which the header 12 is arranged at the beginning of the encrypted multimedia data stream this arrangement of the header and the payload data block is not to refer to the transmission of the encrypted multimedia data stream. The term "header" is only meant to express that a decryption device which is to decrypt the encrypted multimedia data stream at first requires at least parts of the header before the multimedia data itself can be decrypted. Depending on the transmission medium the header may also be arranged at some place in the payload data block or be received after certain parts of the payload data block when for example a packet-oriented transmission of the multimedia data stream is thought of, in which different packets, one of

15

25

30

35

5 in an only exemplary way. The header includes as it is shown in Fig. 2 a so-called crypt-block 29 comprising, in general terms, relevant information for encrypting the multimedia data. In addition the header 12 includes a so-called license block 30 comprising data referring to how a user can or is allowed to use the encrypted multimedia data stream. The header 12 further includes a payload data info block 32 which can include information concerning the payload data block 14 and as well as general information about the header 12 itself. Furthermore the header 12 may comprise an old header block 34 enabling a so-called recursive header structure. This block makes it possible for the user who, apart from a decryption device is also in the possession of an encryption device to reformat an encrypted multimedia data stream for other replay instruments in his possession without losing or modifying the original header information provided by the distributor. Depending on the application further sub blocks, such as an IP information block (IP = intellectual property) according to ISO/IEC 14496-1, MPEG-4, Systems, 1998, containing copyright information, can be added to the header 12.

As it is the standard in the art, an internal block structure can be allocated to each block, this structure at first requesting a block identifier and including the length of the sub block and at last giving the block payload data itself. Thus, the encrypted multimedia data stream, and in particular the header of the encrypted multimedia data stream, is given an increased flexibility in such a way that it can react to new requirements in such a way that additional sub blocks may be added or existing sub blocks may be omitted.

5 Fig. 3 gives an overview of the block payload data of the individual sub blocks shown in Fig. 2.

At the beginning the crypt block 28 is explained. It contains an entry for a multimedia data encryption algorithm
10 40 identifying the symmetrical encryption algorithm used in the preferred embodiment, which has been used when encrypting the multimedia data. The entry 40 can be an index for a table in such a way that, after reading the entry 40, a decryption device is capable of selecting this encryption al-
15 gorithm the encryption device has used from a plurality of encryption algorithms. The crypt block 28 further includes the entry first step 26, the entry step 24 and the entry amount 22, which has already been illustrated in connection with Fig. 1. These entries in the header enable a decryp-
20 tion device to subdivide an encrypted multimedia data stream accordingly to be able to carry out a correct decryption.

The crypt block 28 further contains an entry for the dis-
25 tributor or provider or supplier 42, the entry being a code for the distributor who has produced the encrypted multimedia data stream. An entry user 44 identifies the user who has obtained the encrypted multimedia data stream in some way from the distributor who is identified by the entry 42.
30 According to the invention it is preferred not to use a person-related user identification since this would open the way for illegal copies. Instead it is preferred to carry out the user identification device specific. The entry user would then for example comprise the serial number
35 of a PC, a laptop, a car hifi system, a home stereo system, smart card etc. that authorizes playing only on a certain device. For further increase of flexibility and/or safety a

5 certain identification like for example a logic link of the
hard disk size with the processor number etc. for the exam-
ple of a PC can be applied instead of a serial number that
looks different for every producer but might by chance be
identical.

10

An entry 46 contains an output value that will be discussed
in detail later. This output value in general represents an
encrypted version of the multimedia data key which, in con-
15 nnection with the multimedia data encryption algorithm iden-
tified by the entry 40, is required to decrypt the en-
crypted multimedia data (sections 16 in Fig. 1) present in
the payload data block 14 correctly. In order to achieve a
sufficient flexibility for future applications, the two en-
tries output value length 48 and output value mask 50 are
20 further provided. The entry output value length 48 illus-
trates the actual length of the output value 46. To achieve
a flexible header format more bytes are however provided in
the header format, for the output value than an output
value actually comprises. The output value mask 50 thus il-
25 lustrates how a shorter output value is distributed in a
way on a longer output value place. If the output value
length is for example half as big as the space available
for the output value, the output value mask could be formed
in such a way that the first half of the output value mask
30 is set while the second half is masked. In this case the
output value would simply be entered into the space pro-
vided for the header by the syntax and occupy the first
half while the other half would be ignored due to the out-
put value mask 50.

35

Now the license block 30 of the header 12 will be ex-
plained. The license block includes an entry bit mask 52.

5 This entry can comprise certain specific information for
replaying or for the general way of using the encrypted
multimedia data. With this entry a decryption device could
especially be told whether the payload data can be replayed
locally or not. In addition at this point it may be sig-
10 nalled whether the challenge response method has been used
for the encryption, this method being described in the al-
ready mentioned German patent DE 196 25 635 C1 and enabling
an efficient data base access.

15 An entry expiration date 54 indicates the point in time at
which the permission to decrypt the encrypted multimedia
data stream expires. A decryption device will in this case
check the entry expiration date 54 and compare it to a
build-in time measuring device in order not to carry out a
20 decryption of the encrypted multimedia data stream if the
expiration date has been exceeded. This makes it possible
for the provider to make encrypted multimedia data avail-
able for a limited amount of time, which has the advantage
of a much more flexible handling and price setting. This
25 flexibility is further supported by an entry starting date
56 in which it is specified from which point on an en-
crypted multimedia file is allowed to be decrypted. An en-
cryption device will compare the entry starting date with
its built-in watch to only carry out a decryption of the
30 encrypted multimedia data when the current point in time is
later than the starting date 56.

The entry allowed replay number 58 indicates how often the
encrypted multimedia data stream can be decrypted, that is
35 replayed. This further increases the flexibility of the
provider in such a way that it for example only allows a
certain number of replays compared to a certain sum which

5 is smaller than a sum which would arise for the unlimited usage of the encrypted multimedia data stream.

For verifying and supporting respectively the entry allowed
replay number 58 the license block 30 further includes an
10 entry actual replay number 60 which could be incremented by
one for example after each decryption of the encrypted mul-
timedia data stream. A decryption device will thus always
check whether the entry actual replay number is smaller
than the entry allowed replay number. If this is the case,
15 a decryption of the multimedia data is carried out. If this
is not the case, a decryption is no longer carried out.

Analog to the entries 58 and 60 entries allowed copy num-
bers 62 and actual copy number 64 are implemented. By means
20 of the two entries 62 and 64 it is made sure that a user of
the multimedia data only copies them as often as he or she
is allowed to do so by the provider or as often as he or
she has paid for when purchasing the multimedia data. By
the entries 58 to 64 a more effective copyright protection
25 is assured, a selection between private users and indus-
trial users being attainable for example by setting the en-
tries allowed replay number 58 and allowed copy numbers 62
to a smaller value.

30 The licensing could for example be designed in such a way
that a certain number of copies (entry 62) of the original
are allowed while copies of a copy are not allowed. The
header of a copy would then, unlike the header of the
original, have zero as the entry allowed copy number in
35 such a way that a proper encryption/decryption device can
no longer copy this copy.

15

25

35

5

The header 12 finally includes the old header block 34, which, along with the synchronizing information, which is not shown in Fig. 3, comprises the entry old header 70. In the entry old header 70 the old header can be maintained by the provider if a user performs an encryption himself and thus produces a new header 12, in order not to lose essential information the provider has entered into the header. For this purpose author information (IP information block) could for example count prior user information and distributor information which enables tracing back of a multimedia file which for example has been decrypted and encrypted several times by different instruments to the original provider transparently, the author information being maintained. It is thus possible to check at any point whether an encrypted multimedia file has been acquired legally or illegally.

Fig. 4 shows a schematic block diagram of a scenario wherein the inventive concept can be applied in an advantageous way. An author or composer 100 has created a multimedia piece, for example a text, a piece of music, a film or a picture. He delivers this work, in this invention generally referred to as multimedia piece, to a supplier 102 of multimedia data. It is especially pointed out here that the expression "multimedia data" in the sense of the present invention comprises audio data, video data or a combination of audio and video data.

The supplier ensures that the multimedia piece of the author/composer 100 is put in circulation by encoding it for example according to the method MPEG layer 3 (MP3). In order to achieve a customer selective providing for use of

5 the encoded multimedia piece the supplier 102 will bring the encoded multimedia piece into a first data stream comprising a header and payload data block. A data stream as it might be used is illustrated in Fig. 3.

10 In this connection it should be especially pointed to the IP information block 72 comprising author information 74 as payload data identifying the author/composer or in general artist. The IP information block could for example be carried out according to ISO/IEC 14496-1 MPEG-4 systems, 1998.

15 It could especially comprise the name of the author/composer/artist or also the ISBN number (ISBN = international standard book number), the ISRC code (ISRC = international standard recording code), the ISAN number (ISAN = international standard audiovisual number), the ISMN number (ISMN = international standard music number), etc. Such

20 meta information will allow a unique identification of the author of the multimedia piece such that by adding these meta information to the payload data the enforcement of copyrights will be much easier.

25

The supplier of multimedia data 102 generates a first data stream comprising a first header and a first payload data block. All the data illustrated in Fig. 3 can be included in the header, wherein the author information (entry 74),

30 the distributor identification (entry 42) and the user identification (entry 44) should be especially noted. While the author information (entry 74) represents the origin of the multimedia piece in general, the distributor identification (42) uniquely defines the origin of the first data

35 stream while the user identification defines the "destination" of the first data stream, i.e. the device that is allowed to use the data stream and that has also paid for it,

5 whereby on the one hand the service of the supplier 102 of multimedia data is paid and on the other hand royalties to the author/composer 100 can flow. In the first header of the first data stream a receiver-PC 104 could for example be identified by the user identification 44. The first data
10 stream can now on the one hand be played on the receiver-PC 104, however, according to the invention, the receiver-PC is defined in such a way that it can also generate a "copy" of the first data stream in order to generate one or several second data streams comprising in their header the user
15 identification 44 of a car hifi system 106a, a home hifi system 106b, a solid state player 106c, etc.

Every second header will essentially comprise the same payload data block, the header of every second data stream,
20 i.e. the second header, will however be different regarding the user identification 44. However, according to the invention, every second header will comprise information allowing conclusions as to the origin of the respective second data stream. This information can comprise author in-
25 formation, an identification for the receiver-PC 104 and an identification for the supplier 102 of the first data stream. Preferably, the second header additionally comprises licence information referring to the fact how often the multimedia piece may be played or how often it may be
30 copied. It can especially happen that for example five copies are allowed but no copy of the copy is allowed. In the entry allowed copy number 62 of the first header there would for example be five. In the entry allowed copy number of the second header however, there would be zero. Even
35 when the car hifi system 106a, the home hifi system 106b or the solid state player 106c were designed in such a way that it can carry out a decryption or an encryption by it-

5 self, i.e. like the receiver-PC 104, still no further copy
would be produced, i.e. no third data stream, since the en-
try 62 in the second header of the second data stream is
set to zero. If this were not the case and if the copy of a
copy were allowed the devices 106a to 106c could again cre-
10 ate third data streams but would comprise origin informa-
tion of the respective second data stream and naturally of
the respective first data stream.

This results in a recursive header structure shown sche-
15 matically in Fig. 5 that can principally be repeated arbi-
trarily. Fig. 5 shows an nth data stream 110 comprising an
nth header 112 and an nth payload data block 114. The nth
header 112 again comprises a (n-1)th header that again com-
prises a (n-2)th header, etc.

20 Preferably, the supplier of multimedia data 102 (Fig. 4)
encrypts the multimedia data in the first payload data
block at least in parts. Preferably, a symmetrical encrypt-
ing method for encrypting the multimedia data is used,
25 wherein the key of the symmetrical encrypting method is
again encrypted asymmetrically. The asymmetric key en-
crypting with the private key of the supplier 102 for the
symmetrical encrypting method is the output value 46 (Fig.
3). The receiver-PC 104 will therefore need the respective
30 public key of the supplier 102 of multimedia data in order
to decrypt the output value 46 again, in order to obtain
the key for the symmetrical decrypting method that the sup-
plier 102 of multimedia data has used as well. The re-
ceiver-PC 104 is now enabled to play the first data stream.
35 If the first data stream is encoded the receiver-PC 104
carries out a decoding prior to playing. The sequence will
therefore be: decrypting, decoding, and playing.

5

However, the receiver-PC should also be able to generate a second data stream for a specific additional player 106a to 106c. In this case the receiver-PC 104 can be configured for encrypting the multimedia data that are decrypted, wherein a symmetrical encrypting method is preferred due to speed aspects. The receiver-PC 104 will again asymmetri-
 10 cally encrypt the key for the symmetrical encrypting method with its private key, provide the second header with its own identification as distributor entry 42 and further provide the second header with the identification for example
 15 of the car hifi system as user identification 44. Further, the receiver-PC 104, will generate a different output value that will be entered into the entry 46 of the second header since the receiver-PC has a different data key than the
 20 supplier 102 of multimedia data. Above that, the receiver-PC will update the licence-block of the second header as desired. However, according to the invention, it will preferably write the whole first header into the entry old header 70 in such a way that all information of the first
 25 header are maintained and especially the origin information of the first data stream as it has been described several times.

Neither the first, second or the nth header are encrypted
 30 themselves. In order to protect the respective headers from attacks after the completion e.g. of the second header a hash sum is formed on the header for example according to a hash algorithm identified in entry 68 (Fig. 3). Preferably, this hash sum is not only formed by the blocks 28, 30, 32,
 35 72 of the second header but it also comprises the block for the old header 34. This hash sum can then be directly entered into the entry 66 (Fig. 3). For the increase of

5 safety it is however preferred to enter a digital signature
for the hash sum of the second header. A digital signature
of the hash sum on the second header could for example be
again formed with an asymmetrical encryption method in such
a way that the receiver-PC 104 generating the second data
10 stream encrypts the hash sum on the second header with its
own private key and writes the result into the entry 66.

The home hifi system 106b will now at first verify the sec-
ond data stream by also forming a hash sum on the second
15 header as it is supplied to the home hifi system. Further,
the home hifi system 106b will decrypt the entry 66 in the
second header with the public key of the receiver-PC 104
and compare the obtained result with the just calculated
hash sum. If both hash sums are the same it can be assumed
20 that the second data stream has not been manipulated. If
the two results differ, a legally implemented car hifi sys-
tem will not continue playing since it can be assumed that
unallowed manipulations have been carried out either at the
second header or in a way "belated" at the first header.

25

Fig. 6 shows a flow chart for the inventive method for gen-
erating a second data stream from a first data stream that
is carried out by the receiver-PC 104 in order to "retag"
the device specifically licensed first data stream to other
30 devices (106a to 106c).

Basically, the receiver-PC 104 will at first extract the
header from the first data stream (116). Above that, the
receiver-PC 104 will generate a second header for the sec-
35 ond data stream (118) as far as possible. This header gen-
erated as far as possible could comprise all information of
the header shown in fig. 3 (blocks 28, 30, 32, 34, 72), but

5 not the old header block 34. This block will be described
in a step 120, wherein at least the origin information from
the first header is entered into the entry 70. However, for
safety reasons and also for implementation reasons it is
10 preferred to enter not only the origin information from the
first header but also all information from the first header
into the entry 70 of the second header. This could lead to
the fact that certain information exist twice, like e.g.
the author information 74 as well as information from other
blocks, for example first step 26, step 24, amount 22, etc.
15 Already here it can be seen that by the fact that the re-
ceiver-PC 104 generates a complete second header in step
118 it is not bound to the parameters of the supplier 102
of multimedia data. For example, a less expensive encrypt-
ing method could be applied in order to enable the second
20 data stream to be encrypted with less effort again for ex-
ample by the solid state player 106c that needs, as known,
limited memory and processor resources in order to be of-
fered inexpensively. Considering these aspects the payload
data block of the second data stream might even not be en-
25 crypted anymore at all, if preferred.

Finally, the receiver-PC 104 generates a second payload
data block for the second data stream (122) in order to fi-
nally obtain the second data stream.

30

The flow chart in Fig. 7 describes in general a method for
playing a second data stream generated based on a first
data stream, wherein this method could be carried out in
one of the devices 106a to 106c. If between the supplier
35 102 of multimedia data and the receiver-PC 104 a further
intermediate distributor as for example a "retailer" of
multimedia data is disposed whom the supplier 102 of multi-

5 media data who will then have a wholesaler function supplies, the inventive method generally illustrated in Fig. 7 would already be carried out by the receiver-PC 104.

10 Generally, the method for playing can be started with the step of reading the second header of the second data stream (130). The device 106a will then for example extract the part of the first header comprising origin information, i.e. the old header block 34 and read the payload data of the entry 70 (132).

15 In order to prevent the playing of illegal pieces the origin of the second data stream is verified in step 134 using the origin information in entry 70. Such a verification could for example consist of checking whether origin
20 information is present in the second header at all (136). If it is found out in the verification 136 that no origin information is present in the second header at all, a legally driven playing apparatus according to the present invention will refuse playing and will stop the operation
25 (138). If it is found out in this simple form of verification 136 that origin information is present and that it makes sense and is no "deception data" of some sort, the inventive playing apparatus will begin or continue playing the second data stream (140).

30 A more expensive way of verification could be to test whether the supplier identification 42 of the second header matches the user identification 44 of the first header. In this case it would be proved without doubt that the copy
35 present in the player comes from the respective home-PC. Any further verification techniques with more or less effort are considered.

5

In a preferred embodiment of the present invention it is preferred to carry out the verification via a digital signature comprising both data of the first header and data of the second header, as it has been described in connection with Fig. 4. Further even more complicated methods can also be used for verification wherein however always the origin of the present data stream is tested that can either be author information or other respective supplier entries 42 or user entries 44 of the individually embedded header of the generally spoken multiply recursive header structure that is illustrated in Fig. 5.

Besides the verification of the origin of the second data stream (step 134 in Fig. 7) the player will preferable be implemented in such a way that it processes also the licence block 30 and especially for example according to the entries 58 and 60 processes regarding to the authorized or actual playing number in order to find out whether it may play a data stream. The player will of course use the other information of the second header in the described manner if the second data stream is encrypted in order to finally decrypt, decode and play the second data stream.